(12) UK Patent Application (19) GB (11) 2 328 310 (13) A

(43) Date of A Publication 17.02.1999

(21) Application No 9709748.9

(22) Date of Filing 14.05.1997

(30) Priority Data
(31) 9610194 (32) 15.05.1996 (33) GB
(31) 9610522 (32) 20.05.1996

(71) Applicant(s)
Ho Keung Tse
PO Box 54670, North Point Post Office, North Point, Hong Kong

(72) Inventor(s)
Ho Keung Tse

(74) Agent and/or Address for Service
Lloyd Wise, Tregear & Co
Commonwealth House, 1-19 New Oxford Street, London, WC1A 1LW, United Kingdom

(51) INT CL^6
G07F 7/10

(52) UK CL (Edition Q)
G4V VAK

(56) Documents Cited
WO 96/00485 A2 US 4797920 A US 4536647 A

(58) Field of Search
UK CL (Edition P) G4V VAK
INT CL^6 G07F 7/10
ONLINE:WPI

(54) Abstract Title
Electronic transaction authorisation system

(57) An electronic transaction and authorisation system comprises a receiver, eg a pager, for receiving information of a transaction to be authorised and a one time, non-predictable code; and for conveying the information and the code to its user. The user, after checking the transaction information is correct, sends the code to an authentication centre directly or through the payee, via an existing communication(s) network system, for authorising the transaction.

GB 2 328 310 A

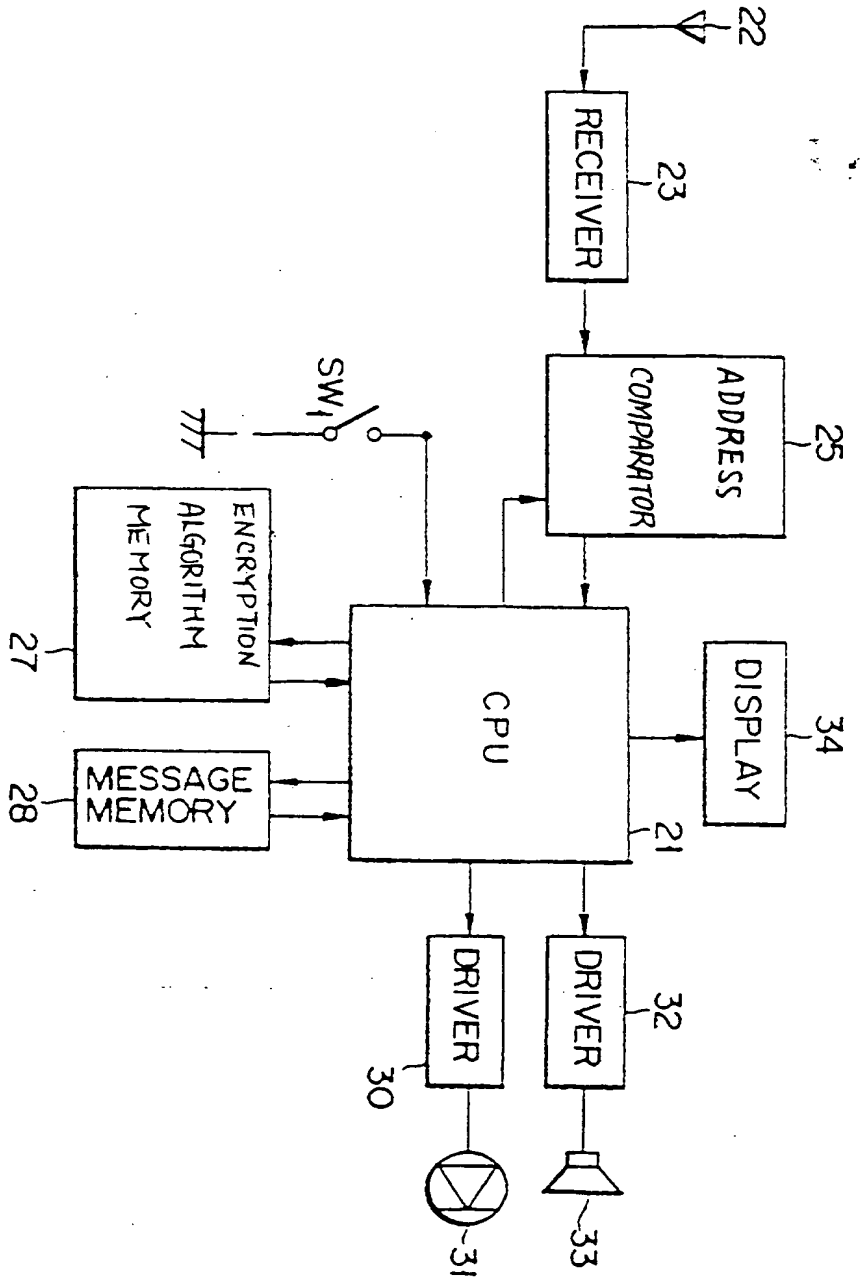
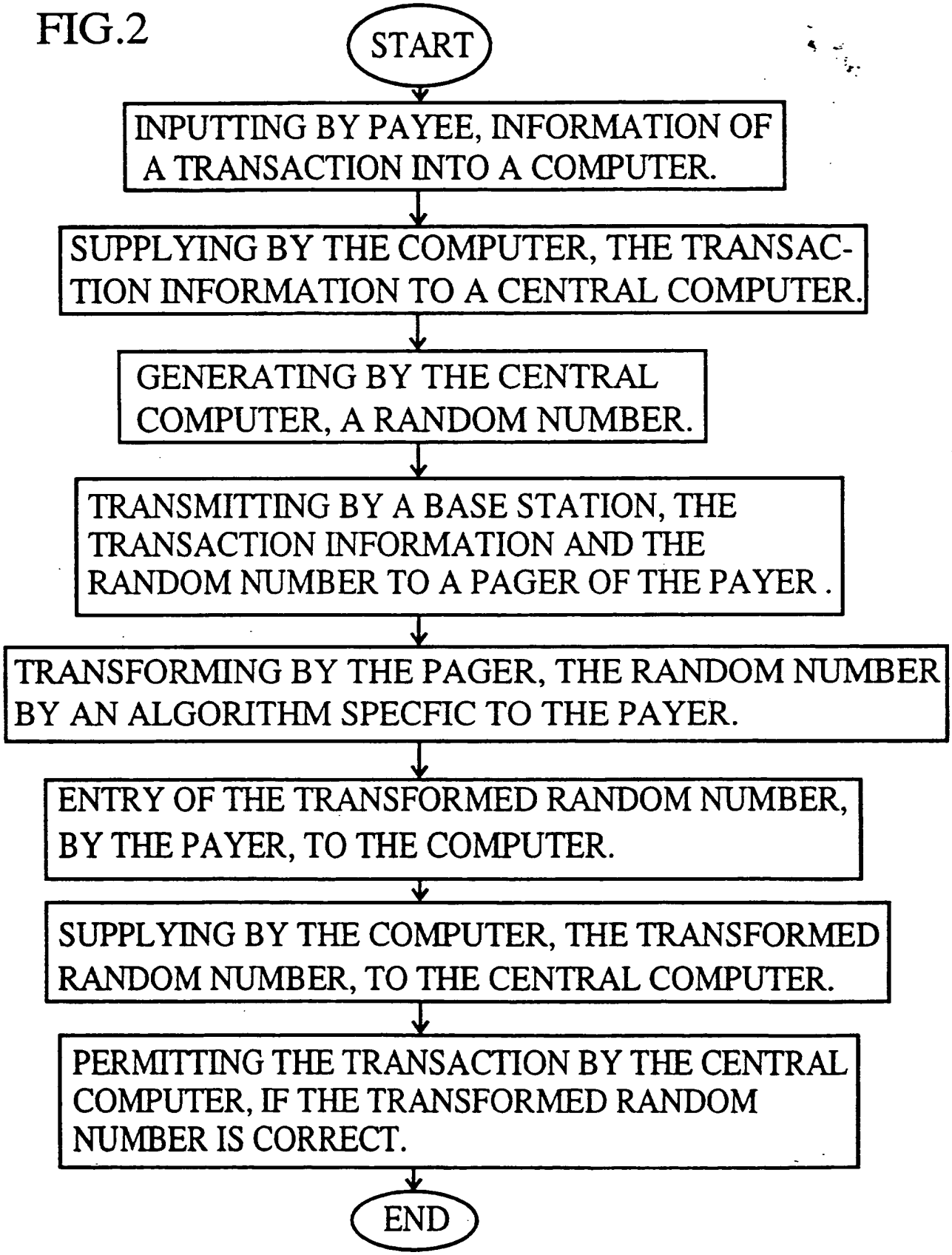


FIG. 1

FIG.2



UNIVERSAL ELECTRONIC TRANSACTION SYSTEM AND METHOD THEREFOR

Field of the invention

The present invention relates to electronic transaction system, and particularly, to an electronic money transaction system with high portability and flexibility for enabling user to effect transactions of any kinds or for any purposes.

Background of the invention

Nowadays, electronic money transaction systems are easily found in the services/products providers such as restaurants and shops for receiving payments. Among such conventional systems, the IC credit card is regarded as a secure means for effecting transactions, and even though, it does have a problem as lacking the capability for providing reliable information about the transaction to be authorised, and as a consequent, it can not be used to ensure a transaction being authorised is exactly the transaction being intended by its holder. Further that, the use of a credit card requires the co-operation of a dedicated terminal, which generally being limited for receiving payments to a particular services/products provider only, and inwhich a number of security problems inherent.

Such a dedicated terminal is necessary for interfacing the IC card and coupling it to a remote central computer which responsible for authenticating the IC card, by establishing a communication link. It should be noted that, the communication link need not be a secure one as far as communication between the IC card and central computer is concerned because when an authentication process take place, the central computer will generate and send a random number to the IC card through the communication link, and the IC card will encrypt the random number and return the encryption result back to the central computer through the communication link. If the encryption result is correct, the central computer will permit the transaction. If a secure communication between the IC card and the central computer is to be used, this

will only mean that the random number will be encrypted one more time, this should be unnecessary and even if it was necessary, it should be carried out by/inside the IC card instead.

In additional thereto, the terminal is also necessary for providing reliable transaction information, particularly, the transaction amount, to the cardholder by means of , for e.g., a display. This means that the terminal has to be a secure device, i.e., it cannot be modified or interfered with. Further, the terminal also has to establish a secure communication link with the central computer to ensure the transaction information communicated thereto cannot be intercepted and modified.

To ensure no card fraud by, for e.g., the cashier of a services/products provider or even the provider itself, a IC card holder has to get into close vicinity of the terminal to monitor the transaction procedure handled by the cashier and desirably, should insert and remove the card into and from the terminal on his own.

In situations where such a terminal does not exist, the IC card will become useless, or it may take the card holder walk a long way if the location of the terminal is remote from the location where the cardholder receives the service/product, this may happen in a shop or restaurant with thousands of sq. ft. in size.

It may also be necessary for a cardholder to get out of his car to make payment for car park fee or fuel intake.

Finally, an I.C. card cannot be used for purchasing in internet environment.

Recently, efforts have been made in developing specialised telephone/internet computer with security functions and capability of interfacing an I.C. card, for enabling people to perform a variety of transactions related to banking and shopping. However, unless all the existing telephones/computers are being replaced by such specialised telephones/internet computers, a cardholder can only expect his I.C. cards will still be basically restricted for making payments to those services/products providers with a dedicated terminal as mentioned above installed.

Objects of the present invention :

Accordingly, it is therefore an object of the present invention to provide an apparatus to a user, rather than the services/products providers, for conveying to the user directly reliable information of a transaction to be authorised, and for enabling the user to authorise that transaction; and a method therefor.

It is therefore another object of the present invention to provide an apparatus to a user, rather than the services/products providers, for enabling a electronic transaction to take place with the aid of any existing general purpose communication(s) network system such as telephone, internet computer or the like, without modification thereof for the security problems as mentioned above; and a method therefor.

It is therefore a further another object of the present invention to provide a universal electronic transaction system which being low cost, secure, not dedicated for any particular purpose; and a method therefor.

Brief description of the invention:

According to one embodiment of the present invention, there is provided a pager for receiving a paging signal representative of information of a transaction, for e.g., on a user account, to be authorised, and representative of a non-predictable code for use by the user to authorise that transaction. The user of the pager, after checking the transaction information including transaction amount and receiver's identity, being correct, sends or gives the non-predictable code to the receiver who will communicate the non-predictable code to the bank for authorising the transaction.

According to another embodiment of the present invention, there is provided a pager with an IC card receiving port therein for receiving an external conventional IC credit card. The pager being for receiving a paging signal representative of information

of a transaction to be authorised and representative of a non-predictable code. The IC card being for transforming the non-predictable code according to an encryption algorithm specified to the user, and the encryption result being for use by the user to authorise that transaction.

Brief description of drawing

FIG.1 is a block diagram of a present paging receiver according to a first embodiment.

FIG.2 is a flow chart of a method for a present authentication process.

Detailed description of the preferred embodiments

Referring to Fig.1, there is shown a block diagram of a paging receiver 1, according to a first embodiment of the present invention, in which comprising :

1) a receiver circuit 23 for receiving paging signals including signals representative of electronic money transaction information (herein below referred as E signals) ;

2) an address comparator 25 for checking whether a signal is assigned to the paging receiver 1 and which may comprise a plurality of addresses for reception of different kinds of signals ;

3) a CPU 21 for fetching a message following the call signal is determined to be assigned to the receiver 1 ;

4) a message memory 28 for storing a received message ;

5) a display 34 for displaying the message received ;

6) a cryptographic algorithm memory 27 for transforming at least a part of the E signals, of which details will be described herein below later ;

7) a speaker 33 and led 31 for providing sound and light signal respectively to a user for indicating a paging signal received .

When in operation, the paging receiver 1 will receive any paging signals transmitted from a base station of the same pager based broadcast system. Such a paging signal contains 4 field, namely as, 1) address field for containing an address of

the paging receiver assigned for receiving the signal ; 2) type field for indicating whether the signal is a E signal or not ; 3) information field for containing information to be displayed to user ; 4) signal number identity for indicating to the paging receiver 1 that, a signal which being broadcasted by the base station more than one time for ensuring it will be received by paging receiver 1 be the same signal, so that pager receiver 1 will ignore the successively identical signals and will not alert the user unnecessarily. The receiving circuit 23, after amplifying the incoming paging signal, supplies the signal to the address comparator 25 which will compare the address field of the signal with one or a number of stored address(es) representative of the user's identity therein, and if a coincidence occurs, the address comparator will feed the rest of the signal to the CPU 21, otherwise, the rest of the signal will be ignored.

According to the first embodiment, the present paging receiver is for to be used to achieve authentication of user identity for a secure operation on a user's account. Referring to Fig.2, which is a flow chart of a method for the authentication process. As read on Fig.2, when an authentication process takes place, an internet computer which desirably has a card reader therein for obtaining the user account number by, for instance, reading a magnetic card or a IC card or the like of the user, otherwise the user account number will have to be entered by hand. Then, it supplies the account number together with the transaction information, which may be entered into the computer with the aid of a keyboard by the payee and which may include information such as identity of payee, transaction amount, purpose of payment, e.g., deposit or full payment for a particular product or service or the like, identity of product(s) and services concerned etc., to a central computer through an existing communication(s) network system which in this case, the internet. The central computer, in response thereto, generates a one time, non-predictable code which being a random number and searches in a user accounts storage thereof the user identity corresponding to the user account number received and then supplies the user identity searched, the transaction information received together with the random number to the base station mentioned

above.

The base station will then search in an address storage thereof an address of the paging receiver of the user, according to the user identity received, and generate a paging E signal, in a format as mentioned above and in which the information field contains the transaction information and the random number, and broadcast the signal.

The paging receiver 1, after receiving the signal, transforms the random number therein by the algorithm stored in cryptographic algorithm memory 27, which being specific to the user, and then alerts the user and displays the transaction information and the transformed random number to the user. The user, after seeing that the transaction information being correct, enters the transformed random number read on display 34 into the keypad of the internet computer which again sends it to the central computer.

The central computer, in response thereto, searches in a cryptographic algorithm storage thereof a corresponding cryptographic algorithm of the user and transforms the random number it generated previously by the cryptographic algorithm searched and compared the result with that of the paging receiver 1, and if the comparison result is favourable, the user's identity is authentic.

It should be noted that the cryptographic process in the paging receiver 1 and the central computer may be omitted to simplify the authentication process and at the same time, it can still provide a acceptable degree of security. This is possible for the reason that although the paging signal can be received by anyone, they can not use it unless they know the correct address of the paging receiver of the user because nowadays, thousands of similar signals may occur and be receivable at the same instant of time.

On the other hand, security of such a system may be enhanced by having the address stored in address comparator 25 be changeable and be changed when a specific paging signal, send by the base station, containing a command of a first predetermined bit pattern and followed by a new address which being encrypted is received. CPU 21,

after receiving such a command, will decrypt the encrypted address by using the encryption algorithm stored in memory 27 and put the decrypted address into the address storage of address comparator 25.

Similarly, the cryptographic algorithm memory may also be updated in this way. Specifically, another specific paging signal containing a command of a second predetermined bit pattern and followed by a new algorithm which being encrypted is used therefor. CPU 21, after receiving such a command, will decrypt the encrypted algorithm by using the original cryptographic algorithm in memory 27 and put the decrypted one into memory 27 for to be used thereafter. Other skills well known to those in the art may well be used for updating the address storage in address comparator 25 or algorithm in memory 27, for instance, a terminal may be included in the paging receiver for interfacing a memory card or a computer or the like for that purpose.

Further, the paging receiver may includes a keypad thereon for receiving, by CPU 21, a password and without it CPU 21 will not perform the cryptographic process. Alternatively, it may also be desirable that once a password is entered, CPU 21 will perform the cryptographic process on the random numbers of E signals received within a predetermined period of time thereafter, or will perform the cryptographic process on the random numbers of any E signals until the total transaction amount authorised thereby exceeds a predetermined value, so that the user need not to enter the password every time a transaction take place.

Further still, to enhance the security of the present system, the E signal may be modified as 2 separate signals, 1) E1 signal which being similar to the E signal as mentioned above, except that it contains no random number therein ; 2) the random number signal for containing the random number which being disguised as an ordinary telephone number. And, the address comparator 25 may contains a specific address dedicated for receiving the random number signal. In the random number signal, there is no type field for indicating to CPU 21 that it being a part of a E signal or the type

field therein will not indicates it as a E signal, instead, the address comparator 25 will interrupt CPU 21 in a specific manner when it detect a random number signal is received, thereby informing CPU 21 of this fact.

According to another embodiment of the present invention, there is provided a pager with an IC card receiving port therein for receiving an external conventional IC credit card. Similar to the first embodiment, the pager is also being for receiving a paging E signal representative of information of a transaction to be authorised on a user's bank account, or the like, and representative of a non-predictable code which being a random number, but in this case, the CPU 21 in the pager will not perform an cryptographic process on the random number, instead, it supplies it to the external IC card in the receiving port. The IC card, upon reception of the random number, will transform it according to an cryptographic algorithm therein, and the result will be communicated to CPU 21 which will cause it, together with the transaction information received, to be displayed in display 34.

It should be noted that, as the user relies on the transaction information received by his pager in making a transaction, it is therefore no longer necessary or a must for the services/products providers to install a dedicated secure terminal as mentioned above. Rather, an existing general purpose communication(s) network system can be used for communicating the transaction information as well as the non-predictable code for authorising the transactions to the central computer.

If merely communicating the account numbers of the money payer and receiver as well as the transaction amount is required, then a dual tone telephone will be sufficient.

If further details of the transaction information is required, such as the purpose of the transaction, e.g. to purchase a Benz, model # 380s, serial # 1234 or even personal loan etc., then the transaction information may be communicated to an operator of the bank, who will be responsible for the data entry of the transaction information by means of a keyboard. In this case, it is desirable that both the money

payer and receiver to have a respective pager of their own for receiving the transaction information and a different one time, non-predictable code for use by them respectively to authorise the transaction, so as to prevent loss to any one of them should there are errors in data entry.

If the transaction is a business agreement or contract, information may be communicated to the central computer by means of an internet computer, as mentioned above.

The most important of all, is of course the central computer should keep a digital record of the transaction information for future reference, for e.g., by internet access. In this way, it is possible to achieve a real "paperless" transaction in which no paper money, no paper receipt or record of the like involved.

It should be noted that the above embodiments are given by way of example only, and it will be obvious to those skilled in the art that various change and modifications may be made without departing from the spirit of the present invention. For instance, the non-predictable code may be transformed by the central computer by means of an encryption process before sending to the pager, and the pager, in this case, will decrypt and display the non-predictable code in its original form to the user, for to be used for enabling the transaction.

Similarly, the transaction information may also be encrypted by the central computer in this way before transmitting to the pager. This can eliminate the possibility of the reception of E signal by the pager be interfered by an extremely strong disturbance signal and the pager be fooled by another fake E signal with the same non-predictable code therein but a false transaction information to deceive the user.

It should further be noted that, in the present electronic transaction system, an existing communication(s) network system is required for the purpose of communicating the non-predictable code or a transformation of it back to the central computer. The term "existing communication(s) network system" used herein above, or in the claims herein below, is intended to be interpreted as not only including the

communication(s) network systems exist now, but also the communication(s) network system which may exist in the future and be applicable for that purpose and at the time in future when the present invention is to be used, it actually exists.

What is claimed is :

1) An electronic transaction apparatus, comprising :

A receiver, comprising :

means for receiving a first signal which being broadcasted for to be received by said receiver and representative of information related to a transaction for to be authorised by said user ,

means for receiving a second signal which being broadcasted for to be received by said receiver and representative of a one time, non-predictable code for use by said user to authorise said transaction ,

means for conveying said information and said code to said user ;

Wherein said one-time, non-predictable code being for to be communicated to an authentication means directly or indirectly through a first existing communication(s) network system and said authentication means will determine said transaction as authorised if receives said one-time, non-predictable code.

2) An electronic transaction apparatus as claimed in claim 1, wherein there is a human operator for communication of said one-time, non-predictable code through said first existing communication(s) network system from another person, and for communication of said one-time, non-predictable code to said authentication means by means of an information entry means.

3) An electronic transaction apparatus as claimed in claim 1, wherein said first signal being in an encrypted form and said receiver will decrypt it before conveying it to said user.

4) An electronic transaction apparatus as claimed in claim 1, wherein said second signal being in an encrypted form and said receiver will decrypt it before conveying it to said user.

5) An electronic transaction apparatus as claimed in claim 1, wherein said one-time, non-predictable code being communicated to said authentication means through said first communication(s) network system which being not dedicated for this purpose.

6) An electronic transaction apparatus as claimed in claim 1, wherein said first existing communication(s) network system being a telephone network and said non-predictable code being entered by means of a dual tone telephone.

7) An electronic transaction apparatus as claimed in claim 1, wherein said first existing communication(s) network system being the internet and said non-predictable code being entered by means of an internet computer.

8) An electronic transaction apparatus as claimed in claim 1, wherein said receiver further comprising a means for receiving an external module for transforming said second signal representative of said one-time, non-predictable code by means of a predetermined cryptographic algorithm specific to said user, thereby obtaining said one time, non-predictable code therefrom.

9) An electronic transaction apparatus as claimed in claim 1, wherein said one-time, non-predictable code being a random number.

10) An electronic transaction apparatus as claimed in claim 1, wherein said means for conveying being a display.

11) An electronic transaction apparatus as claimed in claim 1, wherein further comprising said authentication means.

12) An electronic transaction apparatus as claimed in claim 1, wherein said transaction being an electronic money transaction on an account under the control of said user.

13) An electronic transaction apparatus as claimed in claim 12, wherein said information related to said transaction is being received by said authentication means through a second existing communication(s) network system directly or indirectly.

14) Apparatus for effecting an electronic transaction, comprising :

means for generating a one time, non-predictable code ;

means for broadcasting a signal representative of information related to a transaction for to be authorised by a user and said code, said signal being for to be received by a receiver means of said user and to be conveyed to said user by said receiver means ;

means for receiving said code through an existing communication(s) network system directly or indirectly ;

means for determining said transaction as authorised if said code is received by said means for receiving.

15) Apparatus as claimed in claim 14, wherein further comprising said receiver means.

16) Apparatus claimed in claim 14, wherein said signal representative of said code being in an encrypted form and said receiver means will decrypt it before conveying it to said user.

17) Apparatus claimed in claim 14, wherein said signal representative of said information being in an encrypted form and said receiver means will decrypt it before conveying it to said user.

18) An electronic transaction system, comprising :

means for receiving information related to a transaction for to be authorised by a user ;

means for generating a one time, non-predictable code ;

means for broadcasting a signal representative of said information and said code for to be received by a receiver means of said user and to be conveyed to said user by said receiver means ;

wherein there is a human operator for communication of said one-time, non-predictable code through a communication network from another person and then communication of said one-time, non-predictable code to said system and said system will determine said transaction as authorised if receives said code.

19) An electronic transaction system as claimed in claim 18, wherein further comprising said receiver means.

20) An electronic transaction system as claimed in claim 18, wherein further comprising :

means for receiving said code from said human operator ;

means for determining said transaction as authorised if receives said code.

21) A method for effecting an electronic transaction, comprising the steps of :

generating, by an authenticating means, a one time, non-predictable code ;

transmitting, by a transmitting means, a signal representative of information related to said transaction and said code, for to be received by a receiver means of said user ;

conveying, by said receiver means, said transaction information and said code to said user ;

Wherein said one-time, non-predictable code being for to be communicated to said authentication means directly or indirectly through an existing communication(s) network system and said authentication means will determine said transaction as authorised if receives said one-time, non-predictable code.

Amendments to the claims have been filed as follows

1) In an electronic transaction apparatus for use in a system having a control means for obtaining first information of proposed transactions from third information at least a part received from a remote 2-way communication device , comprising :
a receiver, comprising :

means for receiving said first information of a first proposed transaction which being caused to be broadcasted in the air by said control means for to be received by said receiver ;

means for receiving second information which being broadcasted in the air for to be received by said receiver, for use in generation of a one time, non-predictable code for use by the user of said receiver to confirm fairness of said first transaction ;

means for conveying said received first information to said user , so as for assuring said user(s) that said control means has obtained correct and sufficient information for defining said first transaction , before said user make said confirmation ;

wherein said user being located at said communication device's location.

2) A apparatus as claimed in claim 1, wherein said first information being in an encrypted form and said receiver will decrypt it before conveying it to said user.

3) An electronic transaction apparatus as claimed in claim 1, wherein said second information being in an encrypted form and said receiver will decrypt it before conveying it to said user.

4) An electronic transaction apparatus as claimed in claim 1, wherein said receiver further comprising a means for receiving an external module for generating said one time, non-predictable code.

5) An electronic transaction apparatus as claimed in claim 1, wherein said one-time, non-predictable code being a random number.

6) An electronic transaction apparatus as claimed in claim 1, wherein said means for conveying being a display.

7) An electronic transaction apparatus as claimed in claim 1, wherein said transaction being an electronic money transaction on an account under the control of said user.

8) Electronic transaction apparatus, comprising :

means for obtaining information of a proposed transaction for to be authorised by a user ;

broadcasting means to broadcast said information in the air, to a receiver means of said user and to be conveyed to said user by said receiver means, so as for assuring said user(s) that said control means has obtained correct and sufficient information for defining said transaction , before said user authorise said transaction .

9) Apparatus as claimed in claim 8 , wherein further comprising said receiver means and said broadcasting means.

10) Apparatus as claimed in claim 3, wherein said information being in an encrypted form and said receiver means will decrypt it before conveying it to said user.

11) An electronic transaction system, comprising :

means for receiving information related to a transaction for to be authorised by a user ;

means for generating a one time, non-predictable code ;

means for broadcasting a signal representative of said information and said code for to be received by a receiver means of said user and to be conveyed to said user by said receiver means ;

wherein there is a human operator for communication of said one-time, non-predictable code through a communication network from another person and then communication of said one-time, non-predictable code to said system and said system will determine said transaction as authorised if receives said code.

12) An electronic transaction system as claimed in claim 11, wherein further comprising said receiver means.

13) An electronic transaction system as claimed in claim 11, wherein further comprising :

means for receiving said code from said human operator ;

means for determining said transaction as authorised if receives said code.

14) A method for effecting an electronic transaction, comprising the steps of :

obtaining, by a control means, first information related to a transaction for to be authorised by a user ;

transmitting in the air, by a transmitting means, second information related to said first information for to be received by a receiver means of said user ;

providing, by said receiver means, said second information to said user, so as for assuring said user(s) that said control means has obtained correct and sufficient information for defining said transaction , before said user confirm fairness of said transaction .

15) An electronic transaction apparatus as claimed in claim 1, wherein said publicly accessible data communication network is a telephone network .

16) An electronic transaction apparatus as claimed in claim 1, wherein further comprising said electronic transaction system.

17) An electronic transaction apparatus as claimed in claim 1, wherein further comprising a broadcasting means for broadcasting said first and second information .

18) An electronic transaction system, comprising :

means for obtaining information related to a transaction for to be authorised by a user ;

means for generating a one time, non-predictable code ;

means for broadcasting said information and information for generating said code to a receiver means of said user ;

means for receiving a code intended for authorisation of said transaction ;

means for determining said transaction as authorised if said means for receiving receives said code.

19) An electronic transaction system as claimed in claim 11, wherein further comprising said broadcasting means.

The Patent Office

22

Application No: GB 9709748.9
Claims searched: All

Examiner: Geoff Nicholls
Date of search: 11 November 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): G4V (VAK)

Int Cl (Ed.6): G07F 7/10

Other: ONLINE:WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	WO 96/00485 A2	(TELEFONAKTIEBOLAGET LM ERICSSON) Whole document relevant, especially pages 12 and 13	1, 5, 6, 10 to 15, 21
A	US 4797920	(STEIN)	
A	US 4536647	(ATALLA)	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.